View metadata, citation and similar papers at core.ac.uk
brought to you by CORE

CIT. Journal of Computing and Information Technology, Vol. 24, No. 1, March 2016, 31–43
doi: 10.20532/cit.2016.1002634

Administrator and Fidelity Based Secure Routing (AFSR) Protocol in MANET

Rohit Singh[1], Himadri Nath Saha[1], Debika Bhattacharyya[1] and Pranab Kumar Banerjee[2]

[1]Department of Computer Science and Engineering, Institute of Engineering & Management, India
[2]Department of Electronics and Communication Engineering, Jadavpur University, India

The proliferation of mobile computing and communication devices are driving a revolutionary change in our information society. Among all the applications and services run by mobile devices, network connections and corresponding data services are without doubt the most demanded services by mobile users. A MANET is a continuously self-configuring, infrastructure-less network of mobile devices connected without wires, which makes it ideal for the present scenario. But, due to lack of any centralized infrastructure and access to trusted authorities, the security in MANET poses a huge threat. The prominent routing protocols we know are generally designed for environments where the nodes within a network are non-malicious. Due to the vulnerable nature of the mobile ad hoc network, there are numerous security threats that disturb its development. We propose a protocol for MANETs named "Administrator and Fidelity Based Secure Routing Protocol" (AFSR), which ensures secure routing through the network: by electing an Administrator node on the basis of Willingness and Fidelity, after which a node only communicates to that secure Admin node. This selection of secured admin nodes results in mitigation of various threats. We have evaluated our proposed protocol by simulating and comparing in GloMoSim.

ACM CCS (2012) Classification: Networks ⟶ Network properties ⟶ Network security ⟶ Mobile and wireless security;
Networks ⟶ Networks protocols ⟶ Network layer protocols ⟶ Routing protocols;
Networks ⟶ Network types ⟶ Ad hoc Networks;
Networks ⟶ Network performance evaluation ⟶ Network simulation

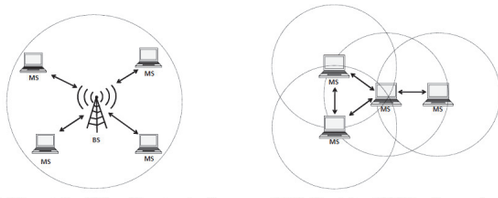
Keywords: MANET, routing, willingness, fidelity, security, attack, proactive, GloMoSim

1. Introduction

An ad hoc network consists of wireless devices that may be mobile and can communicate without the need of a fixed infrastructure. In a Mobile Ad Hoc Network (MANET), the network topology may change dynamically since nodes can move in an unpredictable manner. Nodes are free to move at any speed in any direction and join or leave the network at any time. In [1] Agrawal and Zeng formally define a MANET as an autonomous system of nodes or Mobile Stations (MSs) connected by a wireless medium.

MANET differs from conventional wireless networks, such as cellular networks and IEEE 802.11 (infrastructure mode) networks. The latter ones are self-containing network nodes, which communicate directly with each other, without relying on centralized infrastructures such as base stations. In a MANET, every node is able to communicate directly with other nodes within its range. Nodes with direct communication are called neighbors. Any pair of nodes not directly connected, can communicate through a path formed by other nodes. MANETs are basically peer-to-peer, multi-hop wireless networks. The established links can be either symmetric, links with the same characteristics in both directions, or asymmetric, links with different characteristics in each direction. Information packets are transmitted in a store-and-forward manner by intermediate nodes, i.e., every node acts as a router.

Figure 1(a), presents an example of a wireless network. Every pair of MSs has to communicate through the BS. Figure 1(b) shows an example of a network in ad hoc mode. MSs within the same range can establish direct communication. Ad hoc networks can operate in isolation or may have gateways to a fixed network.



(a) A base station (BS) and its network cell. (b) Mobile stations (MS) in ad hoc mode

Figure 1. Examples of a cellular and an ad hoc network.

MANET can be broadly classified into 3 sections Proactive, Reactive and Hybrid, as reviewed in [2]. The decentralized nature of MANETs provides additional robustness against the single point of failure in centralized approaches, e.g., base stations or access points. MANETs can be deployed in scenarios where it is almost impossible to set up and maintain a wired network, like in the case of a disaster, battlefield or rescue operation. Some limitations of MANET, such as distributed network, dynamic topology, limited bandwidth, energy constraint and limited physical security, make routing in MANET a big challenge. We try to solve these problems through our proposed protocol – An Administrator and Fidelity Based Secure Routing (AFSR).

AFSR can be used in any application where security is a major issue since it has many advantageous features compared to other existing secure routing protocols. In AFSR each node in the network selects only one node as an Admin, from its neighbor table, which will be responsible for its data traffic. Through the process a secure and reliable Admin node is selected, which minimizes the chances of packet drops. As compared to OLSR [3], which selects a set of MPR nodes, AFSR selects a single ADMIN node on the basis of Willingness and Fidelity values, as explained in Section 3. Since the willingness is a combination of the battery, coverage and link stability of the neighbor nodes, it decreases the chances of loss of packets. Moreover, these criterion helps us predict a node which can transfer data from source to destination with high Packet Delivery Fraction and low End-to-End Delay.

Energy efficiency is a challenge in networks like MANET, where the nodes are highly mobile, and frequent route building is required. Our protocol also includes the remaining battery power of a node as a decisive factor for Admin section. Moreover, by selecting only one secure node as an Admin, we minimize the unnecessary multicast of packets to multiple Admins.

Traditional proactive protocols maintain large routing tables, with multiple paths from itself to all potential destination nodes. While doing so, a node also considers some unsecure paths, through which the packets will eventually get lost. AFSR aims to minimize this arduous task of maintaining a big routing table, by selecting the most secured paths and a single reliable Admin node.

The rest of the paper is organized as follows. In Section 2 we review the existing secure routing protocols. In Section 3 we explain the AFSR model, followed by the overall algorithm in Section 4. In Section 5 we explain the results and discussion followed by conclusion in Section 6.

2. Related Work

In recent times, many secure protocols have been proposed to meet up with the different kinds of attacks, as mentioned in [4]. The proposed secure protocols can be broadly classified into four sections as mentioned in Figure 2 [5].

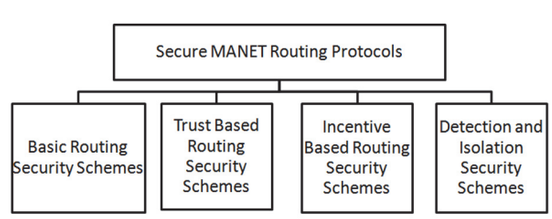


Figure 2. Classification of secure MANET Routing Protocols.

The basic routing security schemes provide authentication services that guard against modification and replaying of routing control messages. However, they do not attempt to provide solutions for issues such as the dropping of packets by selfish or malicious nodes.

In [6] an inter-router authentication scheme for securing AODV [7] routing protocol against external attacks was introduced. The scheme is based on the assumption that the nodes in the network mutually trust each other and it employs public key cryptography for providing the security services. SRP [8] assumes the existence of a security associate between a node initiating a route request query and the sought destination. SAODV [9] uses two mechanisms to secure AODV: digital signatures to authenticate non-mutable fields of the routing control messages and one-way hash chains to secure hop count information, which increases the overhead. ARAN [10] uses digital certificates to secure the routing control messages. ARAN has solved for some attacks, but it is silent about some attacks like black hole attack, denial of service attack, etc. ARAN requires extra memory, it has high processing overhead for encryption, and does not use hop count, so the discovered path may not be optimal. All the above mentioned protocols have not considered battery as a parameter for choosing a secured node, hence making them less reliable. OLSR is vulnerable to wormhole attack, but through Secure OLSR [11], wormhole detective mechanism and authentication are employed to strengthen the neighbor relationship establishment. It uses hash-chain and digital signature to protect the routing packets. However, the number of Admin nodes selected is high. SEAD (Secure Efficient Ad hoc Distance vector routing protocol) [12] has presented a design based on DSDV [13], which uses one-way hash chains for authenticating the hop count values. It uses authentication mechanisms like TESLA, HORS or TIK for authenticating the sender. With the help of message authentication codes it is able to authenticate the sender's routing messages; however, the disadvantage is that it is based on the assumption that shared secret keys are established among each pair of nodes and the nodes should have time synchronized clocks. I-SEAD [14] protocol is an improvement over the SEAD protocol, but still fails to solve the QoS related issues. ARIADNE [15] secures DSR protocol [16]. The routing messages are authenticated by message authentication codes. This demands time synchronization hardware, such that the release of the secret keys can be synchronized. For broadcasting RREQ packets it uses TESLA broadcast authentication protocol distributed to all the nodes through a key distribution center. The advantage is that it uses shared key and digital signature to authenticate messages. It can even detect changes in the node list due to the online central key distribution service. The disadvantage is that attacks like cache poisoning cannot be prevented and the key exchange is a very complicated and heavy process. SPAAR (Secure Position Aided Ad hoc Routing Protocol) [17] is a scheme which was designed to consider a hostile environment. The transmission procedure is quite similar to that of ARAN, and requires that each node has a GPS locator with it to determine its position. The packets are only accepted between neighboring nodes one hop away from each other. A central server generates certificates for authentication. The disadvantage is that the server needs to be uncompromised; moreover, it uses GPS locator, which demands extra hardware.

The trust based secure routing schemes assign quantitative or qualitative trust values of the nodes in the network, based on observed behavior of the nodes. The trust values are used as additional metrics for the routing protocols. SDAR [18] utilizes a trust management system which assigns trust values to nodes based on observed behavior of the nodes, along with recommendations from other nodes. SDAR requires each node to construct two symmetric keys, and shares one with its neighbors that have high trust value and the other with its neighbors that have medium trust values. Protection against packet dropping is not provided by [19]. SLSP's [20] security considerations are limited to individual Byzantine attackers. The protocol is not secure when challenged by two or more colluding nodes. Similarly, ATSR [21] and SMRR [22] have provided a secured approach by employing proactive routing, where the most trustworthy node is selected. In both protocols battery has not been considered during selection of a trustworthy node. Moreover, in SMRR more than one nodes are chosen as Admin, which is not so in this protocol. SAR (Security-Aware Ad Hoc Routing) [23] classifies nodes based on their trust level. Nodes that have the same classification share a secret group key. SAR augments the routing process using hash digests and symmetric encryption mechanisms. The signed hash digests provide message integrity, while the encryption of packets ensures their confidentiality. SAR's advantage is that it will

find the optimal route, such that all the nodes on the shortest path satisfy the security requirements. Its disadvantage is that it may fail to find the route if the ad hoc network does not have a path on which all nodes on the path satisfy the security requirements in spite of being connected. TSRF (Trust-Aware Secure Routing Framework) [24] is a lightweight and trust based scheme to deal with attacks. It tries to combine the trust value with the other QoS metrics. It works well in dense networks and to mitigate greyhole attacks. It does not deal with the energy constraint and it cannot mitigate other attacks like wormhole and byzantine.

The incentive based security scheme presents a brief description of proposed schemes which attempt to stimulate cooperation among selfish nodes by providing incentives to the network nodes. In [3] an incentive-based system for stimulating cooperation in MANETs has been proposed. The scheme requires each network node to have a tamper resistant hardware module called security module. The security module maintains a counter, called nuglet counter, which decreases when a node sends a packet as the originator, and increases when a node forwards a packet. Sprite: A Simple, Cheat-Proof, Credit-Based System for MANETs [25], provides incentive for MANET nodes to cooperate and report actions honestly. Sprite requires a centralized entity called Credit Clearance Service (CCS) which determines the charge and credit involved in sending a message. However, these schemes require tamper resistant hardware and on-line access to a centralized entity; therefore, these schemes are limited in their applications.

The detection and isolation secure scheme removes malicious nodes from the network effectively. In [26] a scheme for mitigating the presence of MANET nodes, that agree to forward packets, but it fails to do so, is presented. The scheme utilizes a "watchdog" for identifying misbehaving nodes and a "pathrater" for avoiding those nodes. However, it might not detect a misbehaving node in the presence of ambiguous collisions, receiver collisions, limited transmission power, false misbehavior, collusion, and partial dropping. A scheme in [27] does not provide protection against false accusations. The techniques in [28], [29] are ineffective against intelligent adversaries, which selectively drop packets, since the probing packets are not completely indistinguishable from other data packets [30]. Modified Dynamic Source Routing Protocol (MDSR) [31] is a non-cryptographic and energy efficient solution for gray-hole attacks. In this protocol, the destination node detects the presence of malicious nodes and isolates them from the network by means of an intrusion detection system IDS. These IDS nodes will only listen in the presence of attack, hence lesser energy loss. However, this scheme does not deal with the battery power of the non-IDS nodes. There can be intelligent malicious nodes which detect these IDS nodes and avoid these nodes. By making few nodes as IDS, it is reducing the resource, hence the traffic on the non-IDS nodes increases eventually taxing their battery power.

3. AFSR Model

In this paper we use Willingness of a node and the Fidelity to select one most secure Admin node, which will be responsible for the transfer of data packets for that node.

3.1. Willingness

Each node, before broadcasting a Neighbor Searching (NS) packet, calculates its own Willingness by Equation 1. The Willingness indicates acceptability of that node to be an administrator. The node receiving this NS packet counts the Willingness of that node to decide its own Admin node.

$$W = f(P,C,S) = (\alpha \cdot P) + (\beta \cdot C) + (\Upsilon \cdot R) \quad (1)$$

Where:

- α, β, Υ are the weight factors of normalization such that Equations 2 and 3 are satisfied.

$$0 < \alpha, \beta, \Upsilon <= 1 \quad (2)$$

$$\alpha + \beta + \Upsilon = 1 \quad (3)$$

- *P:* is the remaining battery power of the node (in %).

$$P = \frac{\text{Current node power}}{\text{Rated capacity of the node}} \cdot 100 \quad (4)$$

- *C:* is the coverage area of the node (in %).

$$C = \frac{\text{No. of 2 hop neighbors} \; - \; \text{No. of 1 hop neighbor which are also 2 hop}}{\text{Total No. of Nodes} - 2} \cdot 100 \qquad (5)$$

The nodes in the neighbor table are known as 1 Hop nodes, while the neighbors of these neighboring nodes are called 2 Hop neighbors. The 2-Hop neighbor node information is received during the Neighbor Searching process, since a node sends its Neighbor Table while broadcasting an NS packet. The coverage area of a node is the measure of a node's ability to reach to other nodes.

- S: is signal stability of the node with all its existing links, measured in dB.

$$S = \frac{\sum_{i=1}^{N} \frac{S_{li} - S_{fi}}{S_{fi}}}{N} \qquad (6)$$

S_{li} and S_{fi} are the last and first signal strength of the i^{th} node respectively, while N is the number of nodes currently present in the neighbor table, since the nodes are present in the neighbor table, $S_{fi} \neq 0$. Moreover, we say that the link with the node is stable if $S_{li} \geq S_{fi}$. The stability of a link will depend on many factors, like distance, pathloss and others. Thus, if we consider the threshold levels of IEEE 802.11b, we can get a range for the numerator in Equation 4. With RADIO-TX-THRESHOLD as -40 dB and RADIO-RX-THRESHOLD as -111 dB [32][33] we get a range from $[-0.65, 1.75]$.

To make these three parameters comparable, we scale these three values on a scale of 10. The three weight factors will depend on different physical conditions [34]. Different types of application have different requirements; hence, the values will change in different circumstances. For our simulation, we have chosen 4 cases CBR, FTP, TELNET and Default (Optimum), as shown in Table 1. We then calculate the best weight factor based on the highest Packet Delivery Fraction (PDF) in GloMoSim.

A bound for the Willingness is necessary to improve the PDF and decrease the number of incapable candidates for Admin selection. We have observed for a simulation environment as mentioned in Section 4, that a node should have at least 30% or above battery value, and at least one 2 Hop neighbor, and has a positive stability to carry on with its task. Considering these minimum requirements, we get the Willingness threshold W_0 as shown in Equation 7.

Table 1. Computed values of weighted parameters.

Case	Weight-factors chosen			PDF	Best Weight-factors chosen		
	α	β	γ		α	β	γ
CBR	0.2	0.2	0.6	0.49	0.5	0.3	0.2
	0.5	0.3	0.2	0.79			
	0.3	0.5	0.2	0.55			
	0.6	0.1	0.3	0.39			
FTP	0.2	0.2	0.6	0.49	0.4	0.3	0.3
	0.5	0.3	0.2	0.59			
	0.4	0.3	0.3	0.61			
	0.2	0.5	0.3	0.45			
TEL NET	0.2	0.2	0.6	0.49	0.3	0.4	0.3
	0.5	0.3	0.2	0.59			
	0.3	0.4	0.3	0.71			
	0.1	0.6	0.3	0.88			
Default	0.3	0.3	0.3	0.8	0.33	0.33	0.33

$$W_0 = 4 \cdot \alpha + \left\lceil \frac{10}{N-2} \right\rceil \cdot \beta + 4 \cdot \Upsilon \qquad (7)$$

3.2. Fidelity

Fidelity [35] is a counter, which keeps track of the number of correctly received and verified acknowledgement packets (ACK). The value increases only if the ACK is received and verified within a time-period, orelse the value decreases. Hence, fidelity can be summarized as a measure of the past behaviour of an Admin node as shown in Equations 8 and 9.

$$\varphi = f\,(\text{Reception of ACK within time } \tau) \qquad (8)$$

Where,

$$\tau = 2 \cdot \text{Average Delay} \; \cdot \; \text{Hop Count} \qquad (9)$$

Initially all nodes have fidelity assigned as 0. This value helps a node to select an Admin node, based on the past activities with that node.

If a node with a high fidelity value suddenly behaves maliciously, then it will take a lot of time for that node to get its fidelity decreased and get replaced by another non-malicious Admin node. Hence, a maximum limit on fidelity must be calculated. Again, a node that repeatedly fails to send ACK packet back to the originator node should not be considered as an Admin node. Similarly, a minimum limit should also be imposed.

a) Maximum Value: With $\varphi_{\max} \epsilon \{1, 3, 5, 7, 9\}$ for 10, 20, 30 nodes we calculated the time required for a node to select a new Admin node, after the previous Admin node with the maximum fidelity starts malicious behavior, as shown in Table 2. It is obvious that the higher the max fidelity, the higher time will be required to decrease its fidelity and choose a new Admin node. In a competitive environment, where majority nodes in the neighbor table have fidelity close to each other, the change in Admin node is quite frequent. Therefore, to see the effect at worst case, we consider a situation where a single node has reached maximum fidelity, while other nodes are yet to start communication, i.e, the fidelity is 0 for other nodes. Let us assume a network with Uniform node placement and with Random waypoint mobility, with the Node Traversal Time $T = 5$ ms. Since our protocol's aim is security, and we would like to isolate the malicious node as fast as possible, we considered the $\varphi_{\max} = 3$, which is evident from Table 2. Moreover, the choice of 1 and 2 will be too fast and harsh for the network.

Table 2. Time required (in ms) to select a new Admin node.

Nodes \ $\varphi_{\max}$	**1**	**3**	**5**	**7**	**9**
10	125	425	650	875	1025
20	500	2125	3300	4600	5150
30	700	2750	4050	5800	6300

b) Minimum Value: With $\varphi \min \epsilon \{-1, -3, -5, -7, -9\}$ for 10, 20, 30 nodes we calculate the PDF, after a node has reached the minimum fidelity, and continues to drop the packets, as shown in Table 3. To maximize security, we would like to isolate the malicious node as soon as possible and with minimum loss in packets. However, due to mobile nature of the nodes, a node can face loss due to constant make and break of links. Therefore, anything within $-5 (= \varphi_{\min})$ is acceptable as it gives a 50% PDF.

Table 3. Packet delivery fraction with different values of $\varphi_{\min}$.

Nodes \ $\varphi_{\max}$	**–1**	**–3**	**–5**	**–7**	**–9**
10	0.8	0.72	0.6	0.4	0.15
20	0.75	0.65	0.51	0.33	0.08
30	0.60	0.60	0.52	0.25	0.05

3.3. Combining Willingness and Fidelity

Since both quantities are important for deciding the choice of an Admin node, our protocol tries to select a node with high Willingness and Fidelity. To do so, we divide both values into two zones, namely High and Low. The preference factor μ is a function of the two parameters as shown in Equation 10.

$$\mu = f(W, \varphi) \tag{10}$$

Our protocol initially checks whether the nodes have Willingness more than the threshold level, so the Willingness value ranging from the threshold value W_0 to maximum value of 10 can be divided into two ranges as shown in Equations 11 and 12.

$$W_{High} \epsilon ((W_0 + \frac{10 - W_0}{2}), 10] \tag{11}$$

$$W_{Low} \epsilon [W_0, (W_0 + \frac{10 - W_0}{2})] \tag{12}$$

We can select the high and low ranges for Fidelity in a similar fashion. We consider the range of fidelity, i.e., $\varphi \epsilon [-5, 3]$, as explained above. Therefore, the high and low levels can be written as Equations 13 and 14. Since, initially all nodes will have fidelity 0, it is considered as a part of low range.

$$\varphi_{High} \epsilon (0, 3] \tag{13}$$

$$\varphi_{Low} \epsilon (-5, 0] \tag{14}$$

With Equations $11 - 14$ we can calculate the preference factor μ as shown in Table 4. The node with the least μ is selected as the Admin node.

Table 4. Preference table.

Preference	Willingness	Fidelity
1	High	High
2	Low	High
3	High	Low
4	Low	Low

A node A with (W, φ) combination as (Low, High) is preferred over a node with (High, Low), since the goal of the protocol is to select the most secure Admin node. If there is a tie, then the node with highest Fidelity is selected. If tie still prevails, then any random node from the competing nodes can be selected.

4. Overall Algorithm

4.1. Admin Selection Process

The overall algorithm starts with a node searching process for its neighbors by broadcasting a Neighbor Searching Packet (NS). This packet has the originator id along with its Neighbor table, and its Willingness. When a node receives this packet, it updates its Neighbor 2-Hop table (i.e. the 2 hop neighbors). The receiving node then, along with its Willingness, broadcasts the NS packet as a response. These NS packets are sent periodically, after a time interval T. This is essential in a mobile network like MANET, where there are constant make and break of links. Hence, the neighbor table, along with the neighbor 2-Hop table, needs to be periodically updated.

After a node receives replies to the NS packet, it starts the Admin selection process. The node with the highest preference factor (i.e., least μ value) is selected as the Admin node. This single node will now be responsible for all the selector node's traffic. The selector node then broadcasts an Admin Packet, so that all the neighboring nodes, including the selected node, come to know about its Admin, and that a bidirectional link exists between itself and the selected Admin node. The process is shown through a flowchart in Figure 3.

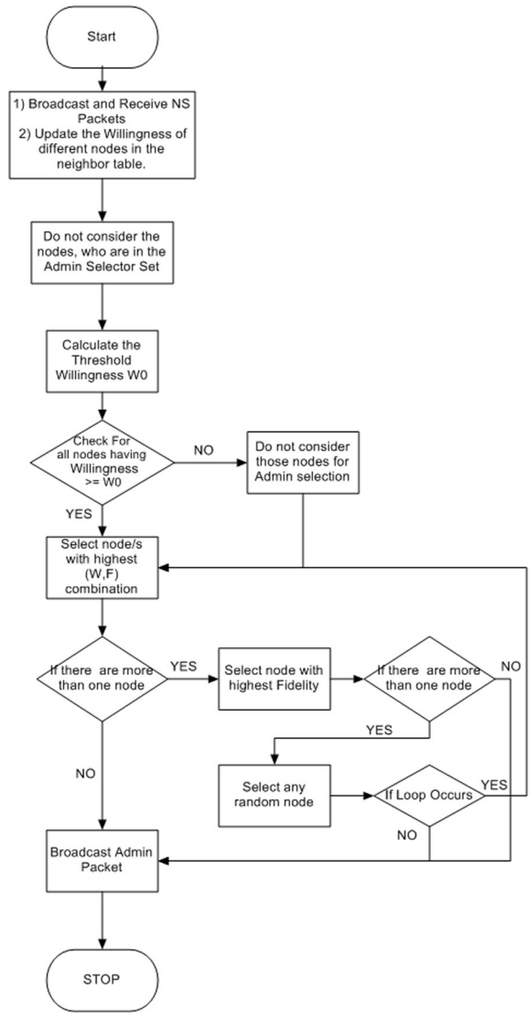


Figure 3. Flowchart for Admin selection.

A node can only have one Admin, but a node can be the Admin of multiple nodes. Therefore, to keep a track of it, an Admin Selector Set is maintained by each node. The node, which is selected as an admin node updates its Admin Selector Set. With each update of this set, a broadcast of the Admin Selector Set Packet is stimulated. The Admin Selector Set packet shares the information about Admin Selector Set of an admin, so that other nodes can update their Connection table and build their routing table accordingly. However, a non-admin neighbor node, on receiving the Admin packet, will also update their Connection Table.

To summarize the Admin selection process, a node needs to consider the following rules:

- A node cannot select a node as an Admin if that node belongs to the Admin Selector Set, thus preventing any kind of parallel edges;
- The node selects only that neighbor node as an Admin, which has the highest preference of Willingness and fidelity combined;
- After selecting an Admin, a node also checks the Connection Table, such that no loop is formed on its choice of Admin. If a loop exists, then the next best Admin is considered.

AFSR selects only one Admin node; hence, the duplication of Admin Selector Set packets is decreased. This packet needs to be digitally signed so that the receiving node can authenticate the information and the identity of the sender. This is essential, as this is the base for creation of the Routing Table. If the Routing table is built based on spurious results generated by malicious nodes, then the whole routing might fail, and the loss of packets will increase a lot.

4.2. Admin Routing

The Connection Table is a collection of all the node and Admin pairs that exist in the network, which a node comes to know through the Admin packet and Admin Selector Set packets. The Routing table is built by tracing these connected pairs, from a potential destination node to itself, through different Admin nodes, as presented in the Connection Table. If X is the destination node, with S as the source and (Y, X), (S, Z), (Z, Y), i.e, (last hop, admin node) are entries in the Connection Table of S, then the path in the Routing Table would be, S→Z→Y→X. The source node now forwards the data packet via the Admin node (in this case node Z) to send it to the destination node (node X).

A source node adds its node id to the MSG.PATH and updates the size of the data packet to reflect the modified path. The node then encrypts the message to be sent with the public key of the destination node so that it can be decrypted only with the private key of the destination node. The sender calculates the HASH value of the encrypted message to ensure whether the actual message is sent to the destination node or not. The sender node maintains a PATHLIST table which also has the HASH value of the encrypted message and the next hop id to keep a record of the node to which it is sending the data for transmission to the destination. It sets a timer and waits for the Acknowledgement (ACK) packet to arrive. If the time out occurs and the sender does not receive an acknowledgement, then it decreases the trust value of the nodes present in neighbor table, and selects a new ADMIN node. The process is shown and explained through a flowchart in Figure 4.

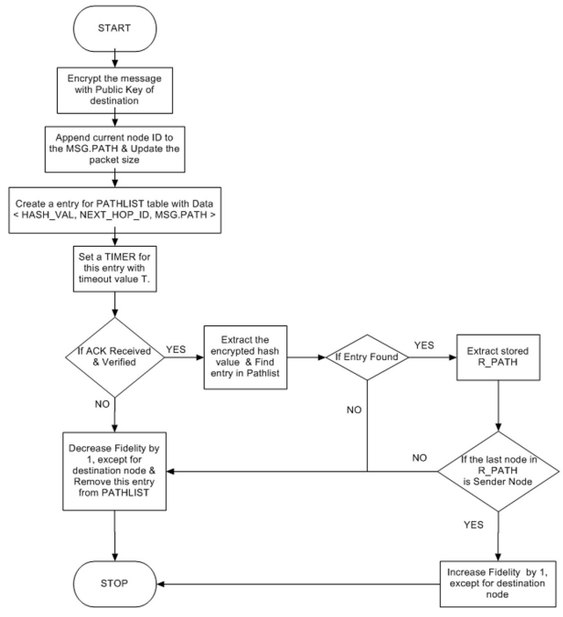


Figure 4. Flowchart for Source node.

On receiving the encrypted message from its previous node, the very first and foremost thing that the node performs is check whether the node from which it receives the message is present in the MSG.PATH. If the node id matches, then it makes an entry to its PATHLIST the Hash value of the message and the NEXT_HOP_ID+MSG. PATH data. It adds its id to the MSG.PATH and updates the message packet size, as to reflect the updated path. Then it forwards the message to its Admin node. If the node id does not match, then it drops the packet and decreases the trust value of the sender node.

This process continues, and when the destination node receives the data, it extracts the PATH from the MSG.PATH of the message. It decrypts the message using its own private key. It now creates a hash value for acknowledgement

generated by hashing the encrypted message, thereby signing the acknowledgement message with its own private key and transmits it to the previous node in the PATH. The ACK packet traces back to the source node through the same path.

On receiving the ACK packet, each of the Admin nodes increases the fidelity of the next-hop (its Admin) by 1, which signifies a successful transmission, otherwise decreases fidelity and the Admin selection is performed again. The process for an Admin is shown in Figure 5.

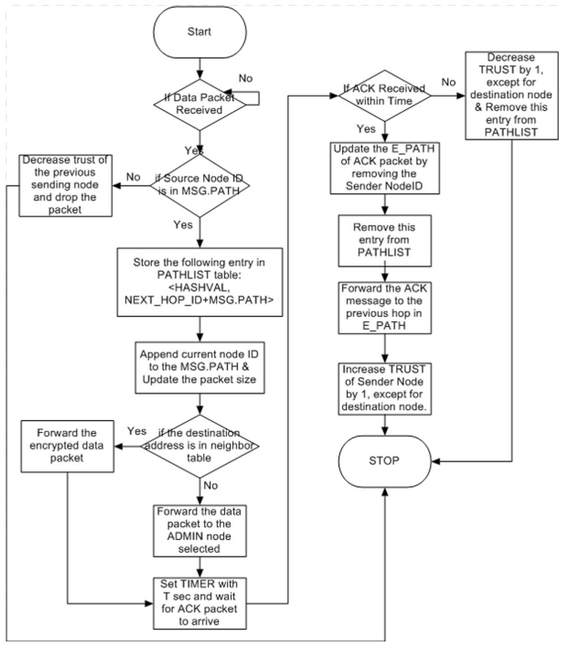


Figure 5. Flowchart for Admin node.

5. Results and Discussions

We have made a comparative study with Secured OLSR, SAODV, ARAN, ARIADNE and our protocol AFSR on Glomosim. We chose these algorithms, since they are all well known secured routing protocols.

The simulation parameters are shown in Table 5. In the simulation, we have considered some assumptions:

- We neglect over-hearing of peer-to-peer packets. The RTS/CTS option is turned off in the MAC layer;
- Any given intermediate node on a path from a source to a destination may be malicious and therefore cannot be fully trusted;
- The source node only trusts a destination node, and a destination node only trusts a source node. So, the source and the destination cannot be malicious;
- We have also used a new self organized key management [36] which uses lesser memory space.

Table 5. Simulation parameters.

Parameters	Values
SIMULATION-TIME	500 seconds
TERRAIN-DIMENSIONS	500m X 500m
NUMBER-OF-NODES	10
NODE-PLACEMENT	UNIFORM
MOBILITY	RANDOM WAYPOINT
MOBILITY-WP-PAUSE	30 seconds
MOBILITY-MIN-SPEED	0
MOBILITY-MAX-SPEED	10 m/s
PROPAGATION-LIMIT	−111.0
PROPAGATION-PATHLOSS	TWO-RAY
NOISE-FIGURE	10.0
RADIO-TYPE	RADIO-ACCNOISE
RADIO-FREQUENCY	2.4 GHz
RADIO-BANDWIDTH	2 000 000 bits/sec
RADIO-RX-SNR--THRESHOLD	10.0 dBm
RADIO-TX-POWER	−10.0 dBm
RADIO-ANTENNA-GAIN	0.0 dB
RADIO-RX-SENSITIVITY	−91.0 dBm
RADIO-RX-THRESHOLD	−81.0 dBm
MAC-PROTOCOL	802.11
ROUTING-PROTOCOL	AFSR, Sec OLSR, ARAN SAODV, ARIADNE
DATA PACKET TYPE	CBR
DATA PACKET SIZE	20 bytes
CRYPTOGRAPHIC ALGORITHM	RSA (512 bit)
SOURCE NODE	NODE 3
DESTINATION NODE	NODE 5
MALICIOUS NODES	30%
$\varphi_{\max}$, $\varphi_{\min}$	$3-5$
α, β, Υ	0.5,0.3,0.2

In Figure 6 we see the average number of Admin node selections throughout the simulation. Since only Secure OLSR uses ADMIN concept, we see that our protocol elects lesser number of Admin nodes. Each node in our protocol selects one node as an Admin, and due to malicious activities these Admins might have to be changed. The average lands to around 1.58 for AFSR. Decreasing the number of Admin nodes selection decreases the routing overhead since lesser broadcast will be required. It even decreases the packet collision at the radio layer.

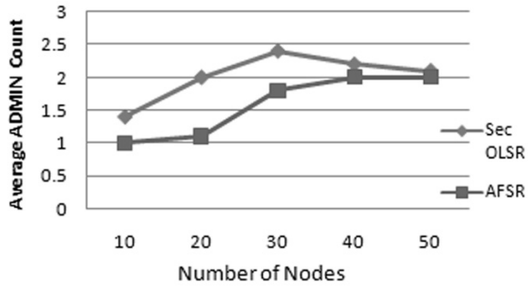


Figure 6. Average ADMIN Count.

The packet delivery fraction (PDF) is the measure of total number of received data packets over total number of sent data packets. In benign environment the packet delivery fraction is slightly lesser than secured OLSR, due to the selection of a single Admin node. However, with fidelity in malicious environment AFSR has a greater PDF. The PDF of AFSR is greater than other secured routing protocols in both environments, since we consider battery, coverage and link stability as essential parameters, while selection of a node is considered an Admin node. Hence, there are greater losses of data packets in ARAN and SAODV, ARIADNE compared to AFSR, as shown in Figures 7 and 8.

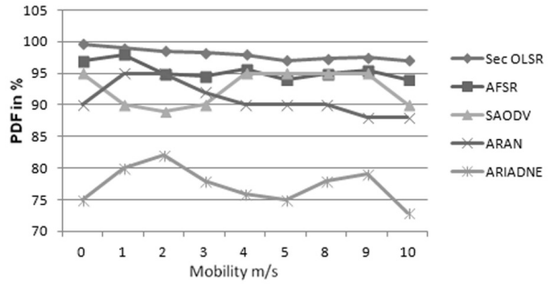


Figure 7. Packet delivery fraction in benign environment.

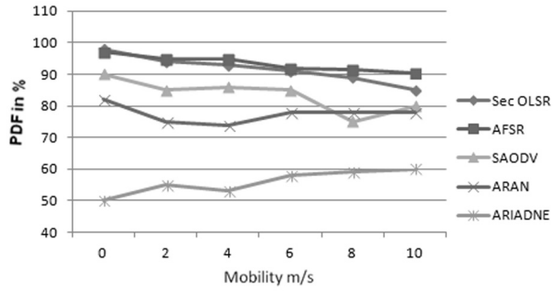


Figure 8. Packet delivery fraction in malicious environment.

The normalized routing load (NRL) is the measure of the number of sent routing packets over the number of received data packets. Lesser Admin node selection helps to decrease the average routing load. Moreover, AFSR has a comparable NRL with respect to other secure on-demand routing protocol in benign environment, as shown in Figure 9. Even in a malicious environment, AFSR maintains a lesser NRL compared to secure OLSR, as shown in Figure 10.

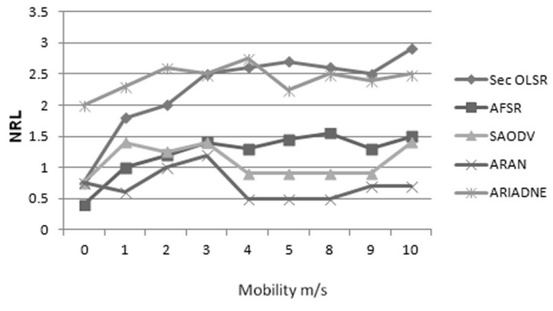


Figure 9. Normalize routing load in benign environment.

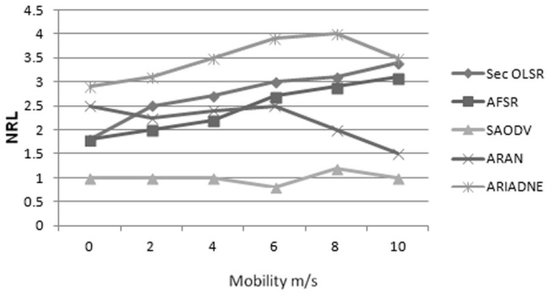


Figure 10. Normalize routing load in malicious environment.

The End-to-End Delay is the average time required for delivering data packets to the destination. AFSR shows the least delay compared to other protocols, since the most reliable routes are selected through willingness, as shown in Figure 11. Moreover, with the introduction of malicious nodes, AFSR maintains an average delay, as shown in Figure 12.

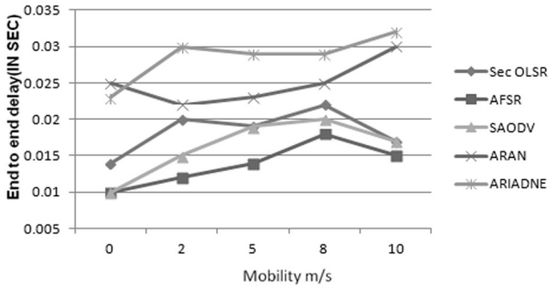


Figure 11. End to End delay in benign environment.

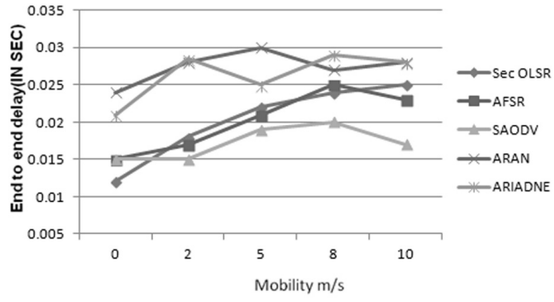


Figure 12. End to End delay in malicious environment.

6. Conclusion

Our presented protocol is a very light-weight routing algorithm and it provides very good security against Black-Hole, gray hole, Jellyfish and Blackmail attacks. While simulating in GloMoSim, we have observed that our protocols work best in a malicious environment as compared to other existing secured protocols mentioned in literature. However, our proposed protocol has a greater End-to-End delay than other protocols, but it has a greater packet delivery fraction (PDF) and lower normalized routing load (NRL) in the same environment. This tradeoff helps in making the protocol secure at a lower cost of packet transmission, lower overhead and lower battery consumption. Due to high dependence on Administrator node and the inherent disadvantages in the proactive type of routing in MANET, this protocol can further be used in reactive protocols, to mitigate their disadvantages.

References

[1] D. P. Agrawal and Q. A. Zeng, *Introduction to Wireless and Mobile Systems*, Boston: Cengage Learning, June, 2010.

[2] H. N. Saha *et al.*, "Review on MANET routing protocols and its vulnerabilities", *International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)*, vol. 2, no. 6, 2013.

[3] B. Awerbuch *et al.*, "An on-demand secure routing protocol resilient to byzantine failures", in *Proceedings of the ACM workshop on Wireless security (WiSE '02)*, 2002. http://dx.doi.org/10.1145/570681.570684

[4] L. Buttyan and J. P. Hubaux, "Stimulating cooperation in self-organizing mobile ad hoc networks", *ACM/Kluwer Mobile Networks and Applications*, vol. 8, no. 5, pp. 579–592, 2003. http://dx.doi.org/10.1023/A:1025146013151

[5] H. N. Saha *et al.*, "A review on attacks and secure routing protocols in MANET, CIBTech", *International Journal of Innovative Research and Review(JIRR)*, vol. 1, no. 2, October–December 2013.

[6] H. N. Saha *et al.*, "Different routing protocols and their vulnerabilities and their measures", in *Intl. Conf. on Advances in Computer Science and Electronics Engineering CSEE 2014*, 2014, pp. 192–202.

[7] L. Venkatraman and D. P. Agrawal, "An optimized inter-router authentication scheme for ad hoc networks", in *Proceedings of the Wireless*, July 2001, pp. 129–146.

[8] C. Perkins and E. Royer, "Ad hoc on-demand distance vector routing", In *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 1999)*, February 1999, pp. 80–100. http://dx.doi.org/10.1109/MCSA.1999.749281

[9] P. Papadimitratos and Z. J. Haas, "Secure Routing for Mobile Ad Hoc Networks", *Mobile Computing and Communications Review*, vol. 6, no. 4, October 2002.

[10] M. G. Zapata, *Secure Ad hoc On-demand Distance Vector (SAODV) routing, IETF MANET Mailing list*, Message-ID 3BC17B40.BBF52E09 @nokia.com, [Online] Available: ftp://manet.itd.nrl.navy.mil/pub/manet/2001-10.mail, 8 October 2001.

[11] K. Sanzgiri *et al.*, "A secure routing protocol for ad hoc Networks", in *Proceedings of 10th IEEE International Conference on Network Protocols (ICNP)*, November 2002. http://dx.doi.org/10.1109/icnp.2002.1181388

[12] F. Hong *et al.*, "Secure OLSR", *in 19th International Conference on Advanced Information Networking and Applications*, AINA 2005, 1, March 2005, pp. 713, 718.

[13] Y. Hu *et al.*, "Sead: Secure efficient distance vector routing for mobile wireless ad hoc networks", In *Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'02)*, 2002, pp. 3–13.

[14] C. Perkins and P. Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (dsdv) for mobile computers", In *Proceedings of the ACM SIGCOMM Conference on Communications Architectures, Protocols and Applications*, 1994, pp. 234–244. http://dx.doi.org/10.1145/190314.190336

[15] W.-S. Lai *et al.*, "I-Sead: A Secure Routing Protocol for Mobile Ad Hoc Networks", *International Journal of Multimedia Ubiquitous Engineering*, vol. 3, no. 4, pp. 45–54, 2008.

[16] Y. Hu *et al.*, "Ariadne: A secure on-demand routing protocol for ad hoc networks", in *Proceedings of the 8th ACM International Conference on Mobile Computing and Networking (Mobicom)*, 2002, pp. 12–23. http://dx.doi.org/10.1145/570645.570648

[17] D. Johnson and D. Maltz, "Dynamic source routing in ad-hoc wireless networks routing protocols, in: *Mobile Computing*, Kluwer Academic Publishers, 1996, pp. 153–181. http://dx.doi.org/10.1007/978-0-585-29603-65

[18] A. Yasinsac and S. Carter, "Secure Position Aided Ad hoc Routing", in *Proceedings of the IASTED International Conference on Communications and Computer Networks (CCN02)*, 2002.

[19] A. Boukerche *et al.*, "An efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc networks", *Computer Communications*, vol. 28, no. 10, pp. 1193–1203, 2005. http://dx.doi.org/10.1016/j.comcom.2004.07.019

[20] A. A. Pirzada and C. Mcdonald, "Establishing trust in pure ad-hoc networks", in *Proceedings of the 27th conference on Australasian computer science (CRPIT'04)*, January 2004, pp. 47–54.

[21] P. Papadimitratos and Z. J. Haas, "Secure Link State Routing for Mobile Ad Hoc Networks", in *Proc. of the IEEE Workshop on Security and Assurance in Ad Hoc Networks*, IEEE Press, 2003, pp. 27–31. http://dx.doi.org/10.1109/saintw.2003.1210190

[22] H. N. Saha *et al.*, "A novel multipoint relay based secure routing in MANET", *International Journal of Network Security & Its Applications (IJNSA)*, vol. 4, no. 6, pp. 133–144, November 2012. http://dx.doi.org/10.5121/ijnsa.2012.4610

[23] A. Banerjee *et al.*, "Administrator and Trust Based Secure Routing in MANET", in *Proceedings of Advances in Mobile Network, Communication and its Applications (MNCAPPS)*, 2012, pp. 39–45. http://dx.doi.org/10.1109/mncapps.2012.13

[24] J. Duan *et al.*, "A Trust-Aware Secure Routing Framework in Wireless Sensor Networks", *International Journal of Distributed Sensor Networks*, 2014. http://dx.doi.org/10.1155/2014/209436

[25] S. Zhong *et al.*, "Sprite: A simple, cheat-proof, credit-based system for mobile ad hoc networks", in *Proceedings of the IEEE INFOCOM*, March 2003. http://dx.doi.org/10.1109/INFCOM.2003.1209220

[26] S. Marti *et al.*, "Mitigating routing misbehavior in mobile ad hoc networks", *Mobile Computing and Networking*, pp. 255–265, August 2000. http://dx.doi.org/10.1145/345910.345955

[27] S. Buchegger and J. Le-Boudec, "Performance analysis of the CONFIDANT protocol", in *Proceedings of the 3rd ACM international symposium on Mobile Ad Hoc Networking and Computing (MobiHoc'02)*, 2002, pp. 226–236. http://dx.doi.org/10.1145/513800.513828

[28] B. Awerbuch *et al.*, "An on-demand secure routing protocol resilient to byzantine failures", in *Proceedings of the ACM workshop on Wireless security (WiSE '02)*, pp. 21–30, September 2002. http://dx.doi.org/10.1145/570681.570684

[29] A. Patwardhan *et al.*, "Secure routing and intrusion detection in ad hoc networks", in *Proceedings of the 3rd IEEE International Conference on Pervasive Computing and Communications (PerCom 2005)*, March 2005, pp. 191–199. http://dx.doi.org/10.1109/percom.2005.38

[30] K. Vishnu and A. J. Paul, "Detection and removal of Cooperative Black/Gray Hole Attack in Mobile Adhoc Networks", *International Journal of Computer Application IJCA*, vol. 1, no. 22, 2010.

[31] R. Sharma and K. Gupta, "Comparison based Performance Analysis ofUDP/CBRand TCP/FTP Traffic under AODV Routing Protocol in MANET", *International Journal of Computer Applications*, vol. 56, no. 15, pp. 28–35, October 2012.

[32] H. N. Saha *et al.*, "Fidelity Based on Demand Secure (FBOD) Routing in Mobile Adhoc Network", *International Journal of Advanced Computer Science and Applications (IJACSA)*, *Special Issue on Wireless & Mobile Networks*, pp. 615–627, 2011.

[33] H. N. Saha *et al.*, "Self-organized key management based on fidelity relationship list and dynamic path", *International Journal of Application and Innovation in Engineering & Management (IJAIEM)*, vol. 3, no. 7, pp. 97–100, July 2014.

[34] M. Mohanapriya and I. Krishnamurth, "Modified DSR protocol for detection and removal of selective black hole attack in MANET", *Journal of Computers and Electrical Engineering*, vol. 40, no. 2, pp. 530–538, 2014.

Received: February, 2015
Revised: November, 2015
Accepted: February, 2016

Contact addresses:
Rohit Singh
Department of Computer Science and Engineering
Institute of Engineering & Management
India
e-mail: roh9singh@yahoo.in

Himadri Nath Saha
Department of Computer Science and Engineering
Institute of Engineering & Management
India
e-mail: him_shree_2004@yahoo.com

Debika Bhattacharyya
Department of Computer Science and Engineering
Institute of Engineering & Management
India
e-mail: bdebika2@yahoo.com

Pranab Kumar Banerjee
Department of Electronics And Communication Engineering
Jadavpur University
India
e-mail: pkbju10@yahoo.com

ROHIT SINGH: He is a student at the Institute of Engineering and Management, graduated B.Tech in Computer Science. His research interest is wireless network.

PROF. HIMADRI NATH SAHA: He graduated from Jadavpur University. He obtained his post graduate degree from Bengal Engineering and Science University. He is Assistant Professor at the Institute of Engineering and Management. His research interest addresses security in MANET.

PROF. (DR.) DEBIKA BHATTACHARYYA: She received her Phd. from Jadavpur University in the dept. of ETCE. She is Head of the Department of Computer Science Engineering at the Institute of Engineering & Management. Her research interest addresses security in MANET.

PROF. (DR.) PRANAB KUMAR BANERJEE: He is a Professor at Jadavpur University in the Dept. of ETCE. His research interest addresses security in MANET.